# Mail.ru

**Building the Internet since 1998**

https://corp.mail.ru · @mailru

| Reports resolved | Assets in scope | Average bounty |
|---|---|---|
| 4555 | 22 | $200-$300 |

**Bug Bounty Program**

Launched on Apr 2014

**Includes retesting** ⓘ **Bounty splitting enabled** ⓘ

Policy Hacktivity Thanks Updates (90) Collaborators

Rewards

| Low | Medium | High | Critical |
|---|---|---|---|
| $150 | $3,000 | $20,000 | $60,000 |

Bounties above are maximum values for the Main program scope. Below is more detailed table.

Accepted languages:
🇬🇧 English
🇷🇺 Русский

All amounts are for reference purposes only. Reward applicability and reward amount may depend on problem severity, novelty, exploitation probability , environmental and other factors. Reward decision is made by Mail.Ru security team for each report individually.

## Mail.ru authentication center, mail, messaging, cloud services, portal, content and news projects:

| Vulnerability | Main Scope | MCS | Biz | ICQ | Content |
|---|---|---|---|---|---|
| Remote code execution (RCE) | **$40000** | **$15000 /$2500*** | **$15000** | **$15000** | **$30000** |
| Injections (SQLi or equivalent) | **$30000** | **$10000** | **$10000** | **$10000** | **$20000** |

| | | | | | |
|---|---|---|---|---|---|
| Local files access and manipulation (LFR, RFI, XXE) without jail/chroot/file type restrictions | $30000 | $10000 | $10000 | $10000 | $20000 |
| RCE in dev. infrastructure / isolated or virtualized single-purpose process (e.g. image conversion) | $7500 | $5000/$1000* | $5000 | $5000 | $10000 |
| SSRF, non-blind (with ability to read reply text), except dedicated proxies | $10000 | $5000 | $5000 | $5000 | $10000 |
| SSRF, blind, except dedicated proxies | $2000 | $2000 | $2000 | $2000 | $1500 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of application critical or highly confidential data (e.g. sessions, accounts, passwords, credit cards, e-mail messages) | $12500 | $10000 | $10000 | $10000 | $15000 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of protected personal data or sensitive client information | $7500 | $5000 | $5000 | $5000 | $6000 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of sensitive application or infrastructure data / role privilege escalation within organization / insecure installation of maintained VM image or software package (MCS)** | $1000 - $7500 | $100 - $5000 | $100 - $5000 | $100 - $5000 | $150 - $6000 |
| Admin / support interface authentication bypass | $3000 | $5000 | $3000 | $3000 | $5000 |
| Admin / support interface blind XSS | $2000 | $2000 | $2000 | $2000 | $3000 |
| Cross-Site Scripting (XSS) on e-mail reading via message content (except AMP) | $2000 | $0 | $0 | $0 | $0 |
| Cross-Site Scripting (XSS) *** | $1000 | $1000 | $500 | $1000 / $0 / $250**** | $0 |

| | | | | | |
|---|---|---|---|---|---|
| Cross-Site Request Forgery (CSRF, Flash crossdomain requests) | **$150 - $1000** | **$150 - $1000** | **$150 - $500** | **$150 - $1000 / $0 / $0 - $250** **** | **$0** |
| Mobile application local account compromise or full data access | **$1000** | **$0** | **$0** | **$1000** | **$0** |
| Remote DoS against mobile or desktop application (persistent/non persistent) | **$0** | **$0** | **$0** | **$300 / $150** | **$0** |
| SDC***** technique bypass for critical projects | **$1500** | **$0** | **$0** | **$0** | **$0** |

** standart remote code execution (RCE) / remote code execution (RCE) using vulnerabilities in open source third-party components (including Open Stack)*
*** verbose error outputs, local installation path disclosure, phpinfo() output, performance counters, etc are not considered as sensitive, reports like these are usually accepted without bounty. Software version disclosure reports are not accepted.*
**** self-XSS, XSS specific to non-common browsers (e.g. IE), blocked by CSP and another vectors without proven script execution are usually accepted without bounty. Unused subdomain takeover is considered under same severity / conditions as parent domain XSS.*
***** bounty for ICQ Web Client / ICQ Web API Sandbox / ICQ Web Portal*
****** SDC is explained here, reports are accepted for SDC-aware domains with critical data (e|m|tel|touch|light|cloud|calendar|biz).mail.ru. SDC bypass is direct or indirect (through SDC-anaware domain) access to product-specific API of these projects without valid sdc/sdcs cookie without access to auth.mail.ru ssdc cookie or valid user's credentials. SDC is web based, attacks via e.g. mobile applications are not considered.*

Vulnerabilities in Android applications are also eligible for Google Play Bug Bounty.

## O2O services

### Citymobil *

| Vulnerability | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|
| Remote code execution (RCE) | **$25000** | **$8000** | **$300 - $3000** |
| Injections (SQLi or equivalent) | **$22000** | **$5000** | **$150 - $1500** |

| | | | |
|---|---|---|---|
| type restrictions) | $22000 | $5000 | - $1500 |
| RCE in dev. infrastructure / isolated or virtualized single-purpose process (e.g. image conversion) | $12000 | $4000 | $100 - $1000 |
| SSRF, non-blind (with ability to read reply text), except dedicated proxies | $12000 | $2000 | $0 - $1200 |
| SSRF, blind, except dedicated proxies | $2000 | $750 | $0 - $250 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of application critical or highly confidential data (e.g. sessions, accounts, passwords, credit cards, e-mail messages) | $18000 | $3000 | $150 - $1500 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of protected personal data or sensitive client information | $12000 | $1500 | $100 - $400 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of sensitive application or sensitive infrastructure data / role privilege escalation within organization ** | $150 - $12000 | $0 - $1500 | $0 - $400 |
| Admin / support interface authentication bypass | $8000 | - | - |
| Admin / support interface blind XSS | $4000 | $1000 | - |
| Cross-Site Scripting (XSS) *** | $0-300 | $150 | $0 |
| Cross-Site Request Forgery (CSRF, Flash crossdomain requests) | $150 - 300 | $100 - $150 | $0 |
| Mobile application local account compromise or full data access | $300 | $150 | - |

* ***Tier 1*** *include preauthentication vulnerabilities and vulnerabilities in public Citimobil interfaces and applications.* ***Tier 2*** *include post-authentication vulnerabilities in city-srv.ru, "taxiserv", "fleet", "corporate", "delivery" and driver api.* ***Tier 3*** *include vulnerabilities in supwork.city-mobil.ru, naumen-test.city-mobil.ru and naumen.city-mobil.ru.*

** *verbose error outputs, local installation path disclosure, phpinfo() output, performance counters, etc are not considered as sensitive, reports like these are usually accepted without bounty. Software version disclosure reports are not accepted.*

*** *self-XSS, XSS specific to non-common browsers (e.g. IE), blocked by CSP and another vectors without proven script execution are usually accepted without bounty. Unused subdomain takeover is considered under same severity / conditions as parent domain XSS.*

| | | | |
|---|---|---|---|
| Remote code execution (RCE) | **$65000** | **$40000** | **$25000** |
| Injections (SQLi or equivalent) | **$55000** | **$30000** | **$23000** |
| Local files access and manipulation (LFR, RFI, XXE) without jail/chroot/file type restrictions) | **$55000** | **$30000** | **$23000** |
| RCE in dev. infrastructure / isolated or virtualized single-purpose process (e.g. image conversion) | **$45000** | **$20000** | **$23000** |
| SSRF, non-blind (with ability to read reply text), except dedicated proxies | **$35000**<br>**$35000** | **$10000** | **$23000** |
| SSRF, blind, except dedicated proxies | **$25000** | **$2000** | **$20000** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of application critical or highly confidential data (e.g. sessions, accounts, passwords, credit cards, e-mail messages) | **$45000** | **$1500** | **$22000** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of protected personal data or sensitive client information | **$40000** | **$400** | **$20000** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of sensitive application or sensitive infrastructure data / role privilege escalation within organization ** | **$150 - $40000** | **$0 - $400** | **$0 - $20000** |
| Admin / support interface authentication bypass | **$30000** | **$500** | **$0** |
| Admin / support interface blind XSS | **$18000** | **$300** | **$0-$300** |
| Cross-Site Scripting (XSS) *** | **$3500** | **$150** | **$0** |
| Cross-Site Request Forgery (CSRF, Flash crossdomain requests) | **$150 - $3500** | **$100 - $150** | **$0** |
| Mobile application local account compromise or full data access | **$300** | **$150** | **$0** |

* ***Tier 1** include preauthentication vulnerabilities and vulnerabilities in public Delivery Club interfaces and applications. **Tier 2** include preauthentication vulnerabilities and vulnerabilities in public ZakaZaka interfaces and applications. **Tier 3** include `tips.delivery-club.ru`, post-authentication vulnerabilities in Delivery Club interfaces, post-authentication vulnerabilities in ZakaZaka interfaces, vulnerabilities in applications for couriers and restaurants.*
*** verbose error outputs, local installation path disclosure, phpinfo() output, performance counters, etc are not considered as sensitive, reports like these are usually accepted without bounty. Software version disclosure reports are not accepted.*
**** self-XSS, XSS specific to non-common browsers (e.g. IE), blocked by CSP and another vectors without proven script execution are usually accepted without bounty. Unused subdomain takeover is considered under same severity / conditions as parent domain XSS.*

| | | | |
|---|---|---|---|
| Remote code execution (RCE) | **$1000** | **$12000** | **$4500** |
| Injections (SQLi or equivalent) | **$500** | **$6000** | **$3000** |
| Local files access and manipulation (LFR, RFI, XXE) without jail/chroot/file type restrictions) | **$500** | **$6000** | **$3000** |
| RCE in dev. infrastructure / isolated or virtualized single-purpose process (e.g. image conversion) | **$500** | **$4000** | **$2000** |
| SSRF, non-blind (with ability to read reply text), except dedicated proxies | **$500** | **$4800** | **$2500** |
| SSRF, blind, except dedicated proxies | **$0** | **$1000** | **$750** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of application critical or highly confidential data (e.g. sessions, accounts, passwords, credit cards, e-mail messages) | **$500** | **$6000** | **$2750** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of protected personal data or sensitive client information | **$250** | **$1600** | **$750** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of sensitive application or sensitive infrastructure data / role privilege escalation within organization * | **$0 - $250** | **$0 - $1600** | **$0 - $750** |
| Admin / support interface authentication bypass | **$250** | **$2000** | **$1000** |
| Admin / support interface blind XSS | **$150** | **$600** | **$500** |
| Cross-Site Scripting (XSS) ** | **$0** | **$0** | **$200** |
| Cross-Site Request Forgery (CSRF, Flash crossdomain requests) | **$0** | **$0** | **$200** |
| Mobile application local account compromise or full data access | **$0** | **$0** | **$0** |

* *verbose error outputs, local installation path disclosure, phpinfo() output, performance counters, etc are not considered as sensitive, reports like these are usually accepted without bounty. Software version disclosure reports are not accepted.*

** *self-XSS, XSS specific to non-common browsers (e.g. IE), blocked by CSP and another vectors without proven script execution are usually accepted without bounty. Unused subdomain takeover is considered under same severity / conditions as parent domain XSS.*

| | Alerts | |
|---|---|---|
| Remote code execution (RCE) | $20000 | $3000 |
| Injections (SQLi or equivalent) | $10000 | $1500 |
| Local files access and manipulation (LFR, RFI, XXE) without jail/chroot/file type restrictions | $10000 | $1500 |
| RCE in dev. infrastructure / isolated or virtualized single-purpose process (e.g. image conversion) | $7500 | $1000 |
| SSRF, non-blind (with ability to read reply text), except dedicated proxies | $4000 | $1200 |
| SSRF, blind, except dedicated proxies | $1000 | $250 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of application critical or highly confidential data (e.g. sessions, accounts, passwords, credit cards, e-mail messages) | $10000 | $1500 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of protected personal data or sensitive client information | $5000 | $400 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of sensitive application or infrastructure data * | $0 - $5000 | $0 - $400 |
| Admin / support interface authentication bypass | $3000 | $500 |
| Admin / support interface blind XSS | $1500 | $150 |
| Cross-Site Scripting (XSS) ** | $200 | $0 |
| Cross-Site Request Forgery (CSRF, Flash crossdomain requests) | $100 - $200 | $0 |

* *verbose error outputs, local installation path disclosure, phpinfo() output, performance counters, etc are not considered as sensitive, reports like these are usually accepted without bounty. Software version disclosure reports are not accepted.*
** *self-XSS, XSS specific to non-common browsers (e.g. IE), blocked by CSP and another vectors without proven script execution are usually accepted without bounty. Unused subdomain takeover is considered under same severity / conditions as parent domain XSS.*

## Educational services

Uchi scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or compromises data outside of project's scope (e.g. personal information) via serverside vector.

expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection).

| Vulnerability | Uchi |
|---|---|
| Remote code execution (RCE) | **$1000** |
| Injections (SQLi or equivalent) | **$500** |
| Local files access and manipulation (LFR, RFI, XXE) without jail/chroot/file type restrictions | **$500** |
| RCE in dev. infrastructure / isolated or virtualized single-purpose process (e.g. image conversion) | **$500** |
| SSRF, non-blind (with ability to read reply text), except dedicated proxies | **$500** |
| SSRF, blind, except dedicated proxies | $0 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of application critical or highly confidential data (e.g. sessions, accounts, passwords, credit cards, e-mail messages) | **$500** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of protected personal data or sensitive client information | **$250** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of sensitive application or infrastructure data * | **$0-$250** |
| Admin / support interface authentication bypass | **$250** |
| Admin / support interface blind XSS | **$150** |

* *verbose error outputs, local installation path disclosure, phpinfo() output, etc are not considered as sensitive, reports like these are usually accepted without bounty. Software version disclosure reports are not accepted.*

## Food services

In Food services scopes only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.

Clientside vulnerabilities (XSS, CSRF) and business logic specific bugs, including privilege escalations within the product are accepted without bounty.
MitM and local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection).

| | | | | |
|---|---|---|---|---|
| Remote code execution (RCE) | $1500 | $750 | $1000 | |
| Injections (SQLi or equivalent) | $750 | $400 | $500 | * |
| Local files access and manipulation (LFR, RFI, XXE) without jail/chroot/file type restrictions | $750 | $400 | $500 | |
| RCE in dev. infrastructure / isolated or virtualized single-purpose process (e.g. image conversion) | $500 | $250 | $500 | |
| SSRF, non-blind (with ability to read reply text), except dedicated proxies | $600 | $300 | $500 | |
| SSRF, blind, except dedicated proxies | $250 | $150 | $0 | |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of application critical or highly confidential data (e.g. sessions, accounts, passwords, credit cards, e-mail messages) | $750 | $400 | $500 | |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of protected personal data or sensitive client information | $400 | $200 | $250 | |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of sensitive application or sensitive infrastructure data / role privilege escalation within organization * | $0 - $400 | $0 - $200 | $0 - $250 | |
| Admin / support interface authentication bypass | $500 | $500 | $250 | |
| Admin / support interface blind XSS | $150 | $100 | $150 | |
| Cross-Site Scripting (XSS) ** | $0 | $0 | $0 | |
| Cross-Site Request Forgery (CSRF, Flash crossdomain requests) | $0 | $0 | $0 | |
| Mobile application local account compromise or full data access | $0 | $0 | $0 | |

** verbose error outputs, local installation path disclosure, phpinfo() output, performance counters, etc are not considered as sensitive, reports like these are usually accepted without bounty. Software version disclosure reports are not accepted.*
*** self-XSS, XSS specific to non-common browsers (e.g. IE), blocked by CSP and another vectors without proven script execution are usually accepted without bounty. Unused subdomain takeover is considered under same severity / conditions as parent domain XSS.*

## Extended scope

Clientside vulnerabilities (XSS, CSRF) and business logic specific bugs, including privilege escalations within the product are accepted without bounty.
MitM and local attacks, user enumeration on registration/recovery, insufficient session expiration, cookies working after logout etc are not accepted unless additional impact is identified

| Vulnerability | Ext. A | Ext. B | Ext. O |
|---|---|---|---|
| Remote code execution (RCE) | $30000 | $8000 | $200 - $1000 |
| Injections (SQLi or equivalent) | $20000 | $4000 | $150 - $500 |
| Local files access and manipulation (LFR, RFI, XXE) without jail/chroot/file type restrictions | $20000 | $4000 | $150 - $500 |
| RCE in dev. infrastructure / isolated or virtualized single-purpose process (e.g. image conversion) | $10000 | $2000 | $150 - $500 |
| SSRF, non-lind (with ability to read reply text), except dedicated proxies | $10000 | $2000 | $0 - $500 |
| SSRF, blind, except dedicated proxies | $1500 | $500 | $0 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of application critical or highly confidential data (e.g. sessions, accounts, passwords, credit cards, e-mail messages) | $15000 | $3000 | $150 - $500 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of protected personal data or sensitive client information | $6000 | $800 | $150 - $500 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of sensitive application or infrastructure data * | $150 - $6000 | $0 - $800 | $0 - $500 |
| Admin / support interface authentication bypass | $5000 | $1000 | $0 - $250 |
| Admin / support interface blind XSS | $3000 | $500 | $0 |

* *verbose error outputs, local installation path disclosure, phpinfo() output, etc are not considered as sensitive, reports like these are usually accepted without bounty. Software version disclosure reports are not accepted.*

| Project | Domain |
|---|---|
| Corporate website | `corp.mail.ru` |
| RB Mail | `rb.mail.ru` |
| Rating | `top.mail.ru` |
| Money | `money.mail.ru` |
| Terra bank | `tbank.mail.ru` |
| Combo | `combo.mail.ru` |
| Notify | `apinotify.mail.ru` |
| Blog | `blog.mail.ru` |
| Youla | `youla.ru`, `am.ru` |
| Check fines | `gibdd.mail.ru` |
| Help | `help.mail.ru` |
| Target | `target.my.com` |
| Tracker | `tracker.my.com` |

## Ext. B Projects

Extended B scope has a projects table for helping you search vulnerabilities.

| Project | Domain |
|---|---|
| Boosty | `boosty.to` |
| Education service geekbrains | `gb.ru` |
| 33 Elephants | `33slona.ru` |
| All Cups | `cups.mail.ru` |
| Warface | `warface.com` |
| Hustle Castle | `hc.my.games` |
| Left of Survive | `lts.my.com` |
| Zero City | `zc.my.games` |

| | |
|---|---|
| Lost Ark | `la.mail.ru` |
| Skyforge | `sf.mail.ru` |
| Space Justice | `sj.my.games` |
| Crossfire | `cfire.ru` |
| Allods | `allods.mail.ru` |
| Evolution 2: Battle for Utopia | `evo2.my.games` |
| Perfect World | `pw.mail.ru` |
| Juggernauts Wars | `jw.my.games` |
| Jungle Heat | `jh.my.com` |
| MGVC | `mgvc.com` |
| Player One | `games.mail.ru` |
| IT Territory | `it-territory.ru` |
| Pushkin Studio | `my.games` |
| Allods Team | `allods.mail.ru` |
| Studio Nord | `my.games` |
| VK Work | `*.vkrabota.ru` (including `*.worki.ru` and `*.iconjob.co`). |
| Whalekit | `my.games` |
| BIT.GAMES | `bit.games` |
| Armata | `armata.my.games` |
| Online .Net Development Championship | `znakcup.ru` |
| Warface | `wf.mail.ru` |

## Atom browser

We want to get high quality reports, so we have 2 different reward categories:
Cat 1. High quality report with PoC
Cat 2. Basic report with description or PoC without description

| | | |
|---|---|---|
| Renderer Remote Code Execution | **$6000** | **$2500** |
| Universal XSS (SOP bypass) | **$4000** | **$1500** |
| Vulnerability in built-in Extensions | **$1500** | **$500** |
| Memory corruption without proof of impact | **$500 - $2000** | $0 |
| Information Leak | **$200 - $1000** | $0 |
| DoS (NULL pointer dereference, infinite loop, stack overflow, OOM) | $0 | $0 |

## Pixonic

Pixonic scope only awards critical serverside and application vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or compromises data outside of project's scope (e.g. personal information) via serverside vector.

| Vulnerability | Pixonic |
|---|---|
| Remote code execution (RCE) | **$8000** |
| Injections (SQLi or equivalent) | **$4000** |
| Local files access and manipulation (LFR, RFI, XXE) without jail/chroot/file type restrictions | **$4000** |
| RCE in dev. infrastructure / isolated or virtualized single-purpose process (e.g. image conversion) | **$2000** |
| SSRF, non-blind (with ability to read reply text), except dedicated proxies | **$2000** |
| SSRF, blind, except dedicated proxies | $500 |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of application critical or highly confidential data (e.g. sessions, accounts, passwords, credit cards, e-mail messages) | **$3000** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of protected personal data or sensitive client information | **$800** |
| Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of sensitive application or infrastructure data * | **$0-$800** |
| Admin / support interface authentication bypass | **$1000** |
| Admin / support interface blind XSS | **$500** |
| Mobile application local account compromise or full data access | **$1000** |

$150

** verbose error outputs, local installation path disclosure, phpinfo() output, etc are not considered as sensitive, reports like these are usually accepted without bounty. Software version disclosure reports are not accepted.*

Last updated on November 25, 2021. View changes

Policy

## Scope rules

**The program's scope is limited to technical vulnerabilities in the company's critical web services or mobile apps. To report problems accessing your account or non-security issues, please contact customers support.**

A list of the projects can be found here:
Mail.Ru: https://mail.ru/all
My.Com: https://my.com/

We will not pay a reward (and we will be really upset) if we detect:

- Physical tampering with Mail.Ru Group's data centers or offices
- Social engineering directed at the company's employees
- Breaking into the company's infrastructure and using the information obtained to report vulnerabilities
- Attempt to access arbitrary user's account or data or another vulnerability post-exploitation not required to demonstrate the bug presence
- Distributed network/request flooding and another resources exhaustion attacks. Automated scanning tools must be limited to 5 request per second (300 requests per minute) to one target host summing up all tools and threads running in parallel and must not exceed 5 parallel requests at the same time (5 threads).

Please **use your own accounts, phone numbers, etc** to conduct your research. Do not try to gain access to others' accounts or any confidential information.

## Re-active protection

Remember you are testing production environment which is being used, supported and monitored. To prevent negative reaction, conduct your research in responsible, less intrusive way and reasonably limit impact from your tests for users, moderators and administrators.
Aggressive security scans and tests may trigger alerts and result in re-active measures being enforced, e.g. account, phone number or IP may be blocked. Automated abuse reporting tools are not used by Mail.ru, but in some cases, if attack resembles the real intrusion attempt manual abuse report may be sent by administrator.
We believe moderation and monitoring processes must not be impacted by bug bounty and security team does not interfere with moderation and abuse reporting decisions for individual cases.

it, or a working proof-of-concept. Video and screenshots can illustrate bug report, but can not replace it.

If you do not describe the vulnerability in sufficient detail, the discovery process is significantly prolonged and that doesn't help anybody. It's also very desirable if researcher can explain how exactly he or she found a given vulnerability.

## How are bug reports examined?

Reports about vulnerabilities are examined by our security analysts. Our analysis is always based on worst case exploitation of the vulnerability, as is the reward we pay.

Reports are reviewed within 15 days (this is a maximum period - we'll probably respond sooner).
If you prefer to remain anonymous, we recommend using an alias when submitting bug reports.

## Participating reports

Only reports reported via bug bounty platform interface may be considered for a bounty. A date/time of report on bug bounty platform is considered as a date/time of the report.

## Duplicate reports

Different exploitation vectors for the same bug or similar bugs may be considered duplicating if security team believes information provided for a single vector/bug is enough to fix all vectors or bugs reported. Report for known or duplicating vulnerability is considered as Duplicate. Duplicate report is not eligible for monetary reward. Report can be either a duplicate of another report from any bug bounty platform or a duplicate of the problem internally tracked by Mail.Ru security team. Usually, access to original report or some information from internal task tracker is provided to reporter of Duplicate. In some cases information may not be provided, if a Duplicate contains less information or less critical exploitation vector than original report.
The report is considered as a duplicated to another report from any bug bounty platform, if there is original report is in "New" or "Triaged" state with an earlier report date/time or lower report number of if it updates the report in "N/A" or "Need more info" state and original report is in "N/A" or "Need more info" state for less than 1 week or sufficient information is provided in original report by researcher since the report is transferred to "N/A" or "Need more info" state.
The report is considered as a duplicate to internal task if there is a task in internal task tracker which is tracked by Mail.Ru security team on the time of the duplicate report.

Also, public 0-day/1-day vulnerabilities may be considered as a duplicate within few days after vulnerability details publication, if vulnerability is known to our team from public sources and we are working to mitigate or patch it.

## Invalid reports

Report in "N/A" or "Need more info" state which is stale in this state for more than a week without sufficient new information provided is considered as invalid and does not participate in bug bounty.

## Reward payment

We will pay you a reward if you are the first person to report a given vulnerability.

Payments are made through HackerOne.

## Vulnerability disclosure

Vulnerability must be disclosed only with accordance with bug bounty platform disclosure policy.
Request for vulnerability disclosure must be submitted via bug bounty platform report interface. We usually disclosure reports within 4 weeks after disclosure request or fixing time, but we can request up to 3 months of additional time before vulnerability details are published. This time is required to distribute the fixed version and check it for regressions.
No vulnerability disclosure, including partial is allowed before vulnerability is disclosed on bug bounty platform.
If any sensitive information including (but not limited to) infrastructure and implementation details, internal documentation procedures and interfaces, source code, user and employees data accidentally obtained during vulnerability research or demonstration must not be disclosed. Intentional access to this information is strongly prohibited.
Mail.ru does not disclosure and do not grant you any rights to disclosure vulnerabilities in 3rd party products or services, unless these rights are explicitly given to you by affected 3rd party.

Last updated on May 23, 2021. View changes

Scopes

## In Scope

| | | | |
|---|---|---|---|
| Other | **Ext. O: Acquisitions, not integrated to Mail.Ru infrastructure and external cloud services**<br>This scope covers services and products related or operated by Mail.ru but hosted outside of Mail.ru infrastructure: fresh and non-integrated acquisitions not mentioned for different scopes, different cloud services and externally hosted solutions. It also covers non-production hosts (e.g. staging and demo installations) of Mail.ru projects in MCS cloud hosting.<br>Extended scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br>Clientside vulnerabilities (XSS, CSRF) and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br>MitM and local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection) | Critical | $ Eligible |

| | | | |
|---|---|---|---|
| | services. | | |
| Other | **Mail.Ru Cloud Solutions (MCS)**<br>`mcs.mail.ru`, `infra.mail.ru` except customer-operated hosts in MCS Hosting networks, delegated and externally hosted domains and branded partner services.<br><br>**IMPORTANT:** We can change the reward in this scope if researcher uses 0day in openstack to exploit the vulnerability in report.<br><br>Reports for customer introduced vulnerabilities in MCS Hosting networks belong to **Hosting Scope** and are considered as informative. | Critical | $ Eligible |
| Other | **Main Scope**<br>Mail.ru Mail for iOS, Mail.ru Mail for Android, Mail.ru Cloud for iOS, Disk-o Cloud application, Mail.ru Cloud for Android, Mail.ru Calendar for Android, Код Доступа Mail.Ru for Android, Код Доступа Mail.Ru for iOS , MyMail for iOS, MyMail for Android, `mail.ru` (without subdomains), `e.mail.ru`, `touch.mail.ru`, `m.mail.ru`, `tel.mail.ru`, `light.mail.ru`, `octavius.mail.ru`, `smtp.mail.ru`, `mxs.mail.ru`, `pop.mail.ru`, `imap.mail.ru`, `cloud.mail.ru`, ` `disk-o.cloud`, `calendar.mail.ru`, `todo.mail.ru`, `calls.mail.ru`, `auth.mail.ru`, `o2.mail.ru`, `account.mail.ru`, `swa.mail.ru`, `id.mail.ru`, `contacts.mail.ru` except delegated and externally hosted domains and branded partner services.<br><br>Bugs common for both Mail.Ru and MyMail application / serverside are usually accepted as a single bug. | Critical | $ Eligible |
| Other | **Ext. A Scope**<br>Productivity, e-commerce, B2B projects at `*.mail.ru`, `*.my.com` and some dedicated project domains, including `corp.mail.ru`, `rb.mail.ru`, `top.mail.ru`, `money.mail.ru`, `tbank.mail.ru`, `combo.mail.ru`, `apinotify.mail.ru`, `blog.mail.ru`, `target.my.com`, `tracker.my.com`, `youla.ru`, `am.ru`, `gibdd.mail.ru`, `help.mail.ru` except delegated and externally hosted domains and branded partner services.<br><br>Extended scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br><br>Clientside vulnerabilities (XSS, CSRF) and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br>MitM and local attacks, user enumeration on | Critical | $ Eligible |

| | | | |
|---|---|---|---|
| Other | **Ext. B Scope**<br>Gaming, entertainment, recruitment, educational services and unlisted projects `*.mail.ru`, `*.my.com`, `*.my.games` unlisted in different scopes and dedicated project domains (`*.vkrabota.ru`, `gb.ru`, `33slona.ru`, `tarantool.io`, `bit.games`, `lootdog.io` and game domains within Mail.Ru infrastructure) except delegated domains, externally hosted projects, acquirements not integrated to Mail.Ru infrastructure and branded partner services. Reports for user introduced vulnerabilities in hosted systems or hosted student projects are considered as informative.<br>Extended scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br>Clientside vulnerabilities (XSS, CSRF) and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br>MitM and local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | Critical | $ Eligible |
| Other | **Delivery Club**<br>Delivery Club and ZakaZaka applications, `delivery-club.ru`, `zakazaka.ru` except delegated and externally hosted domains and branded partner services. | Critical | $ Eligible |
| Other | **ICQ**<br>**ICQ web client:** `web.icq.com`<br>**ICQ web portal:** `icq.com`, `icq.im`, `agent.mail.ru`<br>**ICQ API Sandbox:** `icq.net` (ICQ API relies on tokens rather than cookies and HTTP auth and is generally resistant to crossite attacks, check the real impact for crossite access before reporting).<br>**ICQ Application (mobile):** ICQ for Android, ICQ for IOS. Reports for Mail.Ru Agent are only accepted if the report is specific to this branded version.<br>**ICQ Application (desktop):** ICQ for Mac, ICQ for Windows, Source code (*source code is not published with every ICQ version and may contain vulnerabilities already patched in version distributed via ICQ site. Only reports for vulnerabilities in latest version distributed via the ICQ site are accepted*).<br>Mail.Ru Agent and MyTeam are derived from ICQ code. Reports for these messengers are only accepted if vulnerability is | Critical | $ Eligible |

| | | | |
|---|---|---|---|
| Other | MY.GAMES App for Android, MY.GAMES App for iOS and MY.GAMES core services: `my.games` (without subdomains), `account.my.games`, `community.my.games`, `profile.my.games`, `store.my.games`, `market.my.games`, `api.my.games`, `ac.my.games`, `*-ac.my.games`, `auth.my.games`, `c.my.games`, `o2.my.games`, `acint.my.games`, `dummy.my.games`<br>Game subdomains do not belong to this scope.<br>MitM and local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | Critical | $ Eligible |
| Other | **DonationAlerts**<br>`donationalerts.com`, `donationalerts.ru` except delegated and externally hosted domains and branded partner services.<br>MitM and local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | Critical | $ Eligible |
| Other | **Foodplex**<br>Foodplex applications, `ucs.ru`, `plazius.ru`, `sberfood.ru`, `sbertips.ru`, `r-keeper.ru`, `rkeeper.ru` except delegated and externally hosted domains and branded partner services.<br>We accept reports on `*.rkcloud.ucs.ru` if they belong to `srv*.rkcloud.ucs.ru` patern. Open port reports on `srv*.rkcloud.ucs.ru` are only accepted if they contain sensitive information.<br>`sandbox-*` API endpoints are externally available sandboxes for integration testing and may lack authentication or have public testing accounts available. These endpoints are not intended to store any sensitive information, any data available via these endpoints is not considered as sensitive. Reports for ability to access these endpoints and information disclosure reports for these endpoints are not accepted. Another critical serverside vulnerabilities (RCE, SQLi, etc) are accepted under bounty conditions of **Ext.O** scope if vulnerability is specific to sandbox API endpoint.<br>Foodplex scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector. | Critical | $ Eligible |

| | | | |
|---|---|---|---|
| | MitM and local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | | |
| Other | **Samokat**<br>`samokat.ru`, `samokat-team.ru`, `samokat.io`, `smart.space` (domain only, smart.space mobile aplication does not belong to Samokat) except delegated and externally hosted domains and branded partner services, `Samokat` and `Dark Store` applications for iOS/Android.<br><br>Samokat scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br><br>Clientside vulnerabilities (XSS, CSRF) and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br><br>MitM and local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | Critical | 💲 Eligible |
| Other | **Content**<br>Content, portal, news projects (without subdomains): `news.mail.ru`, `sportmail.ru`, `pogoda.mail.ru`, `hi-tech.mail.ru`, `auto.mail.ru`, `hi-chef.ru`, `kino.mail.ru`, `tv.mail.ru`, `lady.mail.ru`, `horo.mail.ru`, `deti.mail.ru`, `dom.mail.ru`, `vseapteki.ru`, `health.mail.ru`, `pets.mail.ru`, `dobro.mail.ru`, `wowsale.ru`, `mediator.media`, `mediator.mail.ru`, `relap.io`, `pulse.mail.ru`, `go.mail.ru`, `browser.ru`, `capsula.mail.ru`, `marusia.mail.ru`, `vc.go.mail.ru`, `otvet.mail.ru`, `smotri.mail.ru`, `dictor.mail.ru`, `home.mail.ru`.<br><br>Content scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br><br>Clientside vulnerabilities (XSS, CSRF), MitM and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br><br>Local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after | Critical | 💲 Eligible |

|  |  |  |  |
|---|---|---|---|
| Other | **Biz**<br>`biz.mail.ru`, `edu.mail.ru` except delegated and externally hosted domains and branded partner services. | Critical | $ Eligible |
| Other | **Uchi**<br>`uchi.ru`, `vchy.com.ua`, `bricsmath.com`, `happynumbers.com`, `happynumbers.com.mx`, `happynumbers.fr`, `happynumbers.es`, `dinolab.in`, `dragonlearn.org`, `dragonlearn.com.br`, `dragonlearn.co.za`, `dragonlearn.in`, `dragonlearn.com`, `zhixuelong.com`, `mathdive.org`, `stagehn.com`, `pluscompetition.com`, `runit.cc` except delegated and externally hosted domains and branded partner services.<br>Uchi scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br>Clientside vulnerabilities (XSS, CSRF), MitM and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br>Local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | Critical | $ Eligible |
| Other | **Citydrive**<br>Citydrive App for Android, Citydrive App for iOS, `citydrive.ru`, `youdrive.today` except delegated and externally hosted domains and branded partner services.<br>Citydrive scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br>Clientside vulnerabilities (XSS, CSRF) and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br>MitM and local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | Critical | $ Eligible |
| Other | **KITCHEN**<br>`localkitchen.ru`, `kak.media` except delegated and externally hosted domains and branded partner services. | Critical | $ Eligible |

| | | | |
|---|---|---|---|
| | Clientside vulnerabilities (XSS, CSRF), MitM and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br>Local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | | |
| Other | **NATIVEROLL**<br>`nativeroll.tv`, `seedr.ru`, `seedr.com` except delegated and externally hosted domains and branded partner services.<br>NATIVEROLL scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br>Clientside vulnerabilities (XSS, CSRF), MitM and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br>Local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | Critical | $ Eligible |
| Other | **Pixonic**<br>War Robots (Windows in Steam and Windows in Amazon), iOS, Android applications, `pixonic.com`, `warrobots.com` except delegated and externally hosted domains and branded partner services.<br>Pixonic scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br>Clientside vulnerabilities (XSS, CSRF), MitM and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br>Local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection). | Critical | $ Eligible |
| Other | **Ext. O: Delegated subdomain or branded partner service** | Medium | $ Eligible |

| | | | |
|---|---|---|---|
| | terms and rules. Researchers must follow rules and service agreement published by resource being investigated. Mail.Ru does not authorize researcher or provide him permissions in any form to research third party resources for vulnerabilities, all permissions must be acquired by researcher directly from third party or partner.<br>Only reports affecting Mail.ru services or customers are accepted.<br>Vulnerability information for third party product or service can not be disclosed within Mail.Ru bug bounty program.<br>Extended scope only awards critical serverside vulnerabilities, if vulnerability compromises the infrastructure (e.g. RCE, SQLi, LFR, SSRF, etc) or data outside of project's scope (e.g. personal information) via serverside vector.<br>Clientside vulnerabilities (XSS, CSRF) and business logic specific bugs, including privilege escalations within the product are accepted without bounty.<br>MitM and local attacks, user enumeration on registration/recovery, open redirections, insufficient session expiration, cookies working after logout etc are not accepted unless there are additional vectors identified (e.g. ability to steal the session token via remote vector for open redirection) | | |
| Executable | **Atom browser**<br>Atom browser is available from https://browser.mail.ru/<br>Atom only accepts vulnerabilities, which affect Atom and do not affect vanila Chromium. How to check if your vulnerability is applicable:<br>1. Launch Chromium current Atom release is based on (check browser://version page).<br>2. Try to reproduce your bug in Chromium and Atom.<br>3. If your bug only affects Atom, create a report. If your bug affects Chromium, check the latest Chromium version and, if it's also affected, send to Chromium bug bounty. | Critical | $ Eligible |
| Other | **Hosting**<br>*3rd party projects and services are not covered by bug bounty terms and rules. Researchers must follow rules and service agreement published by hosted resource being investigated. Mail.Ru does not authorize researcher or provide him permissions in any form to research third party resources for vulnerabilities, all permissions must be acquired by researcher directly from third party / Mail.Ru customer.*<br>User-introduced vulnerabilities in hosted services (Mail.Ru hosting / colocation networks, "Infra" / MCS public cloud | None | $ Ineligible |

projects (e.g. demo product installations, staging hosts, proxy servers, etc) including ones hosted in MCS Hosting networks are covered by **Ext.O Scope**.

MCS hosting infrastructure, default installations and interfaces are covered by **MCS Scope**.

Hosting network can be identified by whois information or PTR name. Customer host in MCS network may have "MCS" in whois description or route information or ###.mcs.mail.ru PTR where ### is last octet from IP address, hosting or colocation networks are usually described as hosting or colocation in whois description. You can use this link to obtain the list of MCS customers networks (requires phone registration for MCS Infra Cloud Computing services).

Alternatively, you can report any vulnerable installations, information on compromised hosts, botnet C&C, and another maliscious/suspicious activity from MCS Hosting networks to abuse@mcs.mail.ru.

Vulnerability information for third party product or service can not be disclosed within Mail.Ru bug bounty program.

## Out of Scope

| | |
|---|---|
| Domain | **love.mail.ru**<br>Report love.mail.ru bugs to Wamba bug bounty program: http://corp.wamba.com/en/developer/security/ |
| Domain | **vk.com**<br>Report VKontakte (vk.com) bugs to https://hackerone.com/vkcom |
| Domain | **ok.ru**<br>Report Odnoklassniki (ok.ru) bugs to https://hackerone.com/ok |
| Other | **We do not accept/review reports with:**<br>• Vulnerability scanners and another automated tools reports<br>• Disclosure of non sensitive information, such as product version<br>• Disclosure of public user information, such as nick name / screen name<br>• Reports based on product/protocol version without demonstration of real vulnerability presence<br>• Reports of missed protection mechanism / best current practice (e.g. no CSRF token, framing/clickjacking protection) without demonstration of real security impact for user or system<br>• Reports regarding published and non-published SPF and DMARC policies<br>• Logout CSRF<br>• Vulnerabilities of partner products or services if Mail.Ru users / accounts are not directly affected<br>• Missed SSL or another BCP for products beyond the main scope<br>• Security of rooted, jailbreaked or otherwise modified devices and applications |

message) if it doesn't lead to UI spoofing, UI behavior modification or another negative impact.
- Same site scripting, reflected download and similar attacks with questionable impact
- CSP related reports for domains without CSP and domain policies with unsafe eval and/or unsafe inline
- IDN homograph attacks
- XSPA (IP/port scanning to external networks)
- Excel CSV formula injection, scripting within PDF documents
- Attack which require full access to local account or browser profile
- Attacks with scenarios where vulnerability in a 3rd party site or application is required as a prerequisite and is not demonstrated
- Theoretical attacks without proof of exploitability
- Denial of Service vulnerabilities
- Ability to send large amount of messages
- Ability to send spam or malware file
- Information disclosure via external references outside of Mail.Ru control (e.g. search dorks to private robots.txt protected areas)
- Disclosure of unused or properly restricted JS API keys (e.g. API key for external map service)
- Ability to perform an action unavailable via user interface without identified security risks

Other

**Reports considered as informative:**

- User-introduced vulnerabilities in hosted services (Mail.Ru hosting network, MCS "Infra" public cloud computing hosts, gaming teams hosting, hosted student works for educational projects, etc)
- Information on compromised accounts of external users for Mail.Ru services

Other

**aliexpress.com / aliexpress.cn**

Report Alibaba (aliexpress.com / cn) bugs to https://hackerone.com/alibaba

View changes Last updated on October 8, 2021.

Response Efficiency

2 days

Average time to first response

2 days

Average time to triage

6 days

Average time to bounty

3 months

Average time to resolution

94% of reports

Meet response standards

Based on last 90 days

Program Statistics

Total bounties paid

$200 - $300

Average bounty range

$2,000 - $55,000

Top bounty range

$162,350

Bounties paid in the last 90 days

534

Reports received in the last 90 days

8 hours ago

Last report resolved

4555

Reports resolved

1498

Hackers thanked

Top hackers

danila

Reputation:2264

pyrk2142

Reputation:2199

byq

Reputation:2164

kwel

Reputation:1923

jayesh25

Reputation:1824

All Hackers